



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/806,667	03/23/2004	Daniel John Bricher	GCSD-1574 (51396)	1170
27975 7590 11/28/2007 ALLEN, DYER, DOPPELT, MILBRATH & GILCHRIST P.A. 1401 CITRUS CENTER 255 SOUTH ORANGE AVENUE P.O. BOX 3791 ORLANDO, FL 32802-3791			EXAMINER PAN, JOSEPH T	
			ART UNIT 2135	PAPER NUMBER
			NOTIFICATION DATE 11/28/2007	DELIVERY MODE ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

creganoa@addmg.com

mn

Office Action Summary	Application No.	Applicant(s)	
	10/806,667	BRICHER ET AL.	
	Examiner	Art Unit	
	Joseph Pan	2135	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED. (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 13 September 2007.
- 2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-34 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-34 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 23 March 2004 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
- ☐ Certified copies of the priority documents have been received.
 - ☐ Certified copies of the priority documents have been received in Application No. _____.
 - ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|--|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413) |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | Paper No(s)/Mail Date. _____ |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO/SB/08) | 5) <input type="checkbox"/> Notice of Informal Patent Application |
| Paper No(s)/Mail Date _____ | 6) <input type="checkbox"/> Other: _____ |

DETAILED ACTION

1. Applicant's response filed on September 13, 2007 has been carefully considered. Claims 1-34 are pending.

Claim Rejections - 35 USC § 103

2. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

3. Claims 1-9, 13-19, 23-34 are rejected under 35 U.S.C. 103(a) as being unpatentable over Dhir et al. (U.S. Patent No. 7,142,557 B2), hereinafter "Dhir", in view of Cheng (U.S. Pub. No. 2003/0221034 A1).

Referring to claim 1:

i. Dhir teaches:

A cryptographic device comprising:

a cryptographic module and a communications module (see figure

8, elements 321 'encryption engine', 301 'wlan transceiver' of Dhir);

said cryptographic module comprising

a user network interface (see figure 8, elements 325 'host bus interface', 326 'host device interface', of Dhir),

a cryptographic processor coupled to said user network interface (see figure 8, element 321 'encryption engine' of Dhir), and

said communications module comprising

a network interface (see figure 8, element 301 'wlan [i.e., wireless local area network] transceiver' of Dhir), and

at least one logic device for cooperating with said cryptographic processor to determine a status of said communications module (see figure 1, element 120 'programmable logic device'; and column 3, lines 1-17 of Dhir).

However, Dhir does not specifically mention that the cryptographic module and the communication module are removably coupled.

ii. Cheng teaches a add-on card for connecting to both wired and wireless networks, wherein Cheng discloses that "The network connection module can be detachable from the add-on card to allow for various network configurations." (see figure 4; and abstract, lines 9-11 of Cheng).

iii. It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of Cheng into the method of Dhir to make the communication module removable from the cryptographic device.

iv. The ordinary skilled person would have been motivated to have applied the teaching of Cheng into the system of Dhir to make the communication module removable from the cryptographic device, because "The network connection module can be detachable from the add-on card to allow for various network configurations." (see figure 4; and abstract, lines 9-11 of Cheng).

Referring to claims 2, 14, 24, 28:

Dhir and Cheng teach the claimed subject matter: a cryptographic device (see claim 1 above). They further disclose a plurality of interchangeable communications modules each for communicating over a different communications media (see figure 4; and abstract, lines 9-11 of Cheng).

Referring to claims 3, 25, 29:

Dhir and Cheng teach the claimed subject matter: a cryptographic device (see claim 1 above). They further disclose the communication module comprising at least one of a type of communication module and an operating status (see figure 4, elements 'ANT2', 'PHY2'; and abstract, lines 6-11 of Cheng).

Referring to claims 4, 26:

Dhir and Cheng teach the claimed subject matter: a cryptographic device (see claim 1 above). They further disclose the logic device (see abstract, lines 1-8 of Dhir).

Referring to claims 5, 15, 31:

Dhir and Cheng teach the claimed subject matter: a cryptographic device (see claim 1 above). They further disclose the indicator (see column 8, lines 27-30 of Dhir).

Referring to claims 6, 16, 32:

Dhir and Cheng teach the claimed subject matter: a cryptographic device (see claim 1 above). They further disclose the complex programmable logic device (CPLD) (see column 1, lines 11-16 of Dhir).

Referring to claims 7, 17, 33:

Dhir and Cheng teach the claimed subject matter: a cryptographic device (see claim 1 above). They further disclose the wireless and wired communications (see figure 4, elements 'ANT2', 'PHY2'; and the abstract, lines 6-11 of Dhir).

Referring to claims 8, 18, 34:

Dhir and Cheng teach the claimed subject matter: a cryptographic device (see claim 1 above). They further disclose the Ethernet (see column 2, line 18 of Dhir).

Referring to claims 9, 19:

Dhir and Cheng teach the claimed subject matter: a cryptographic device (see claim 1 above). They further disclose the processor and the encryption circuit (see figure 8, elements 324 'baseband processor', 321 'encryption engine' of Dhir).

Referring to claim 13:

i. Dhir teaches:

A cryptographic device comprising:

a cryptographic module and a communications module (see figure 8, elements 321 'encryption engine', 301 'wlan transceiver' of Dhir);

said cryptographic module comprising

a user local area network interface (LAN) (see figure 8, elements 325 'host bus interface', 326 'host device interface'; and column 6, line 66-column 7, line 3 '...These are wireless local area network specifications.', of Dhir),

a cryptographic processor coupled to said user local area network interface (see figure 8, element 321 'encryption engine' of Dhir), and

said communications module comprising

a network LAN interface (see figure 8, element 301 'wlan transceiver' of Dhir), and

at least one logic device for cooperating with said cryptographic processor to determine at least one of a type of communications module and an operating status thereof, said at least one logic device also permitting said cryptographic processor to configure said network LAN interface (see figure 1, element 120 'programmable logic device'; and column 3, lines 1-17 of Dhir).

However, Dhir does not specifically mention that the cryptographic module and the communication module are removably coupled.

ii. Cheng teaches a add-on card for connecting to both wired and wireless networks, wherein Cheng discloses that "The network connection module can be detachable from the add-on card to allow for various network configurations." (see figure 4; and abstract, lines 9-11 of Cheng).

iii. It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of Cheng into the method of Dhir to make the communication module removable from the cryptographic device.

iv. The ordinary skilled person would have been motivated to have applied the teaching of Cheng into the system of Dhir to make the communication module removable from the cryptographic device, because "The network connection module can be detachable from the add-on card to allow for various network configurations." (see figure 4; and abstract, lines 9-11 of Cheng).

Referring to claim 23:

i. Dhir teaches:

A communications method comprising:
coupling a cryptographic module to a network device (see figure 8, element 321 'encryption engine' of Dhir);
providing a communications module, a network LAN interface, and at least one logic device (see figure 8, element 301 'wlan [i.e., wireless local area network] transceiver', element 300 FPGA [i.e., field programmable gate array], of Dir);
using the network LAN interface to communicate with a network (see column 6, line 66-column 7, line 3 of Dhir); and
causing the at least one logic device to cooperate with the cryptographic processor to determine a status of the communications module (see column 3, lines 1-17 of Dhir).

However, Dhir does not specifically mention that the cryptographic module and the communication module are removably coupled.

ii. Cheng teaches a add-on card for connecting to both wired and wireless networks, wherein Cheng discloses that "The network connection module can be detachable from the add-on card to allow for various network configurations." (see figure 4; and abstract, lines 9-11 of Cheng).

iii. It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of Cheng into the method of Dhir to make the communication module removable from the cryptographic device.

iv. The ordinary skilled person would have been motivated to have applied the teaching of Cheng into the system of Dhir to make the communication module removable from the cryptographic device, because "The network connection module can be detachable from the add-on card to allow for various network configurations." (see figure 4; and abstract, lines 9-11 of Cheng).

Referring to claim 27:

- i. Dhir teaches:
A communications system comprising:

a plurality of network devices coupled together to define a network, and a cryptographic device coupled to at least one of said network devices (see figure 9 of Dhir);

said cryptographic device comprising a cryptographic module coupled to said at least one network device, and a communications module (see figure 8, element 321 'encryption engine', element 301 'wlan transceiver' of Dhir);

said cryptographic module comprising a cryptographic processor coupled to said user network interface (see figure 8, element 321 'encryption engine', element 325 'host bus interface', element 326 'host device interface' of Dhir);

said communications module comprising a network communications interface, and at least one logic device for cooperating with said cryptographic processor to determine a status of said communications module (see figure 8, element 301 'transceiver', element 300 FPGA [i.e., field programmable gate array] of Dhir).

However, Dhir does not specifically mention that the cryptographic module and the communication module are removably coupled.

ii. Cheng teaches a add-on card for connecting to both wired and wireless networks, wherein Cheng discloses that "The network connection module can be detachable from the add-on card to allow for various network configurations." (see figure 4; and abstract, lines 9-11 of Cheng).

iii. It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of Cheng into the method of Dhir to make the communication module removable from the cryptographic device.

iv. The ordinary skilled person would have been motivated to have applied the teaching of Cheng into the system of Dhir to make the communication module removable from the cryptographic device, because "The network connection module can be detachable from the add-on card to allow for various network configurations." (see figure 4; and abstract, lines 9-11 of Cheng).

Referring to claim 30:

Dhir and Cheng teach the claimed subject matter: a communications system (see claim 27 above). They further disclose configuring the network communications (see column 1, lines 7-9 of Dhir).

4. Claims 10-12, 20-22 are rejected under 35 U.S.C. 103(a) as being unpatentable over Dhir et al. (U.S. Patent No. 7,142,557 B2) in view of Cheng (U.S. Pub. No. 2003/0221034 A1), and further in view of Klein (U.S. Patent No. 6,857,076 B1).

Referring to claims 10, 20:

i. Dhir and Cheng teach the claimed subject matter: a cryptographic device (see claim 1 above). Dhir further discloses the encryption engine (see figure 8, element 321 'encryption engine' of Dhir).

However, they do not specifically mention the data buffer.

ii. Klein teaches data security for digital data storage, wherein Klein discloses the data buffer (see column 5, lines 57-67 of Klein)

iii. It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of Klien into the method of Dhir and Cheng to utilize the data buffer for encryption.

iv. The ordinary skilled person would have been motivated to have applied the teaching of Klien into the system of Dhir and Cheng to utilize the data buffer for encryption, because data buffer can be used to store data during encryption process.

Referring to claims 11, 21:

Dhir, Cheng and Klein teach the claimed subject matter: a communications system (see claim 10 above). They further disclose the tampering (see column 7, line 44-45 of Klein).

Referring to claims 12, 22:

Dhir, Cheng and Klein teach the claimed subject matter: a communications system (see claim 10 above). They further disclose the disabling (see column 10, lines 1-3 of Klien).

Response to Arguments

5. Applicant's arguments filed September 13, 2007 have been fully considered but they are not persuasive.

Applicant argues:

"As such, there is no need to have the transceiver located otherwise than on the same circuit board as the FPGA, which is exactly where Dhir et al. puts it. Yet, the proposed modification would potentially result in a more expensive and complicated removable connection configuration between the transceiver and the FPGA that is simply not necessary." (see page 4, 3rd paragraph, Applicant's Arguments/Remarks).

Examiner maintains:

Dhir discloses "Referring to FIG. 6, there is shown an exemplary embodiment of an FPGA 300 in accordance with one or more aspects of the present invention. FPGA 300 comprises programmable gates 307, programmable input/output (I/O) blocks 306 and transceiver (physical layer) 301. Transceiver 301 may be a 5 GHz radio for purposes of implementing IEEE 802.11a technology or HiperLAN2 technology. It should be understood that both IEEE 802.11a and HiperLAN2 use the same physical layer, and thus transceiver 301 may be used for both technologies. Transceiver 301 physical layer is therefore for Orthogonal Frequency Division Multiplex (OFDM) in accordance with the mentioned technologies. In order to achieve throughput necessary

for operating a 5 GHz radio, transceiver 301 is hardwired or embedded, as opposed to having substantial functionality provided by programmable gates 307. Transceiver 301 is programmably coupled to programmable gates 307 through programmable I/O blocks 306." (see column 7, lines 4-22 of Dhir, emphasis added).

Dhir further discloses "Programmable gates may be programmed to comprise several modules, namely medium access control and baseband controller module 302, encryption algorithms module 305, baseband processor module 324, and host interface(s) module 304, as well as glue and other logic module 303." (see column 7, lines 22-27 of Dhir, emphasis added).

Therefore, Dhir discloses that the transceiver 301 [i.e., transmission module] supports multiple platform, such as IEEE 802.11a technology or HiperLAN2 technology, and is coupled with the FPGA 300 [i.e., encryption module]. However, Dhir does not disclose that the transceiver 301 [i.e., transmission module] is removable from the FPGA 300 [i.e., encryption module].

On the other hand, Cheng teaches an add-on card for a computer which is detachable from the computer and allows the compute to communicate with both wired and wireless networks, wherein Cheng discloses "After the first portion 51A is connected to the second portion 51B, the access control circuit MAC2 will control the wireless transmission module 64 and antenna circuit ANT2 to be connected to the wireless network 30A. The access control circuit MAC2 can also control the connecting circuit PHY2 to be connected to the wired network 30B via the network transmission line 58. The advantage of having the network connection module 68 **removable** is that users can change the network connection module based on changing requirements." (see page 3, paragraph [0030], lines 1-10 of Cheng, emphasis added).

Dhir teaches using a single transmission module to support multiple transmission technologies [i.e., IEEE 802.11a technology or HiperLAN2 technology]. Cheng also teaches using a single transmission module to support multiple transmission technologies [i.e., wireless or wired]. Therefore, Cheng's teaching of using a removable transmission module could be used to enhance Dhir's system so that

"users can change the network connection module based on changing requirements."
(see above).

Conclusion

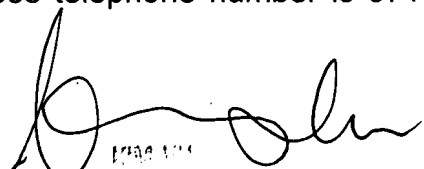
6. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire **THREE MONTHS** from the mailing date of this action. In the event a first reply is filed within **TWO MONTHS** of the mailing date of this final action and the advisory action is not mailed until after the end of the **THREE-MONTH** shortened statutory period, then the shortened statutory will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than **SIX MONTHS** from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Joseph Pan whose telephone number is 571-272-5987.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached at 571-272-3859. The fax and phone numbers for the organization where this application or proceeding is assigned is 703-872-9306.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is 571-272-2100.


SUPERVISOR
TECHNICAL STAFF 100